(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
9 juin 2005 (09.06.2005)

PCT

(10) Numéro de publication internationale
WO 2005/053263 A2

(51) Classification internationale des brevets⁷ : H04L 29/06

(21) Numéro de la demande internationale :
PCT/EP2004/053116

(22) Date de dépôt international :
26 novembre 2004 (26.11.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03104412.6 27 novembre 2003 (27.11.2003) EP

(71) Déposants *(pour tous les États désignés sauf US)* : NAGRACARD S.A. [CH/CH]; Route de Genève 22, CH-1033 Cheseaux-sur-Lausanne (CH). SWISSCOM MOBILE AG [CH/CH]; Schwarztorstrasse 61, CH-3050 Berne (CH).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : KSONTINI, Rached [CH/CH]; Route Aloys Fauquez 26, CH-1004 Lausanne (CH). CANTINI, Renato [IT/CH]; Route du Moulin 35, CH-1782 Belfaux (CH).

(74) Mandataire : WENGER, Joel; Leman Consulting S.A., Route de Clémenty 62, CH-1260 Nyon (CH).

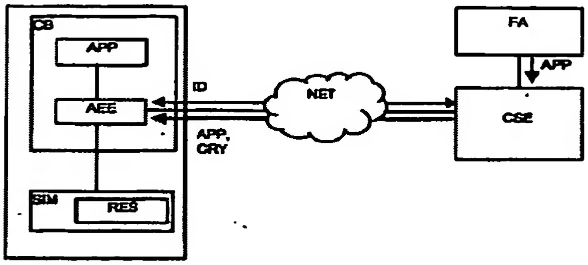
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH,

[Suite sur la page suivante]

(54) Title: METHOD FOR THE AUTHENTICATION OF APPLICATIONS

(54) Titre : MÉTHODE D'AUTHENTIFICATION D'APPLICATIONS



(57) Abstract: The invention relates to a method for managing application security carried out with the aid of a security module associated with mobile equipment. The inventive method authenticates at least one application (APP) functioning in equipment (CB) which is connected by a network (NET) to a control server (CSE), said equipment (CB) being locally connected to a security module (SIM), said application (APP) being loaded and/or run by means of an application running environment (AEE) for the equipment (CB) and utilizing resources (RES) stored in the security module (SIM), comprising the following preliminary stages: receipt of data comprising at least one identifier (IMEISV) of the equipment (CB) and the identifier (IMSI) of the security module (SIM), via the network (NET), by the control server (CSE); analysis and verification by the control server (CSE) of said data; generation of a cryptogram (CRY) comprising an application (APP) imprint (FIN1) of data identifying the equipment (CB) and the security module (SIM) and instructions (INS RES) for said module; transmission of the cryptogram(CRY), via the network (NET) and equipment (CB), to the security module (SIM); verification of the application (APP) by comparing the imprint (FIN1) extracted from the cryptogram (CRY) received with an imprint (FIN2) which is determined by the security module (SIM). The inventive method is characterized in that, during initialization and/or activation of the application (APP), the security module (SIM) carries out the instructions (INS RES) extracted from the cryptogram (CRY) and releases or respectively blocks access to certain resources (RES) of said security module (SIM) according to the result of the verification, which is proper to said application (APP) and which was previously carried out.

[Suite sur la page suivante]

WO 2005/053263 A2